



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,090	03/31/2004	Anthony J. Nadalin	RSW920030288US1	7250
43168	7590	04/15/2008	EXAMINER	
MARCIA L. DOUBET LAW FIRM PO BOX 422859 KISSIMMEE, FL 34742			GERGISO, TECHANE	
		ART UNIT	PAPER NUMBER	
		2137		
			NOTIFICATION DATE	DELIVERY MODE
			04/15/2008	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mld@mindspring.com

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/814,090	NADALIN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	TECHANE J. GERGISO	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 31 March 2004.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-21 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-21 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date 03/31/2004.

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.  
 5) Notice of Informal Patent Application  
 6) Other: \_\_\_\_\_.

## DETAILED ACTION

1. This is non-Final Office Action in response to the applicant's communication filed on March 31, 2004.
2. Claims 1-21 have been examined and are pending.

### *Specification*

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 18 recites "the computer product embodied on one or more computer-readable media." "Computer-readable media" lacks proper antecedent basis in the specification.

### *Claim Rejections - 35 USC § 112*

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
5. Claim 19 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 19 recites the following element "determining how the security-sensitive portions of the message **should** be protected, according to the determined access rights." The recited element renders the claim indefinite and ambiguous to define **the scope and boundary of the claim** because "**how**" and "**should**" suggests an implicitly requirement of active steps instead of

**positively reciting the actual active required steps** to protect the security sensitive portion of a message which are implied by “**how**” and “**should**” language in the claim.

### ***Claim Rejections - 35 USC § 101***

6. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 17 and 18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 17 recites “A system for achieving context-sensitive confidentiality”. Use of the word “**system**” does not inherently mean that the claim is directed to a **machine**. Only if at least one of the claimed elements of the system is **a physical part of a device** can the system as claimed constitute part of a device or a combination of devices to be a **machine** within the meaning of 101. Therefore, claim 17 is rejected as a system of **Software per se**, failing to fall within a statutory category of invention. This is evident in the applicant's disclosure that the invention may take entirely a form of software (see paragraph [0093] recited below):

*[0093] As will be appreciated by one of skill in the art, embodiments of the present invention may be provided as methods, systems, or computer program products. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment combining software and hardware aspects. Furthermore, the present invention may take the form of a computer program product which is embodied on one or more computer-readable storage*

*media (including, but **not limited to**, disk storage, CD-ROM, optical storage, and so forth) having computer-usable program code embodied therein.*

Claim 18 recites “**the computer product embodied on one or more computer-readable media**” and “computer-readable program code **means for**” in the body of the claim. Even though Applicant has invoked the rebuttable presumption that 35 USC 112, 6<sup>th</sup> paragraph applies in the “structure” in the disclosure is not automatically and inherently limited to hardware-inclusive embodiments. It is entirely possible for the corresponding disclosed “means for” to cover an embodiment of the software alone (see paragraph [0093] recited above). Therefore, claim 18 is rejected as a **Software per se**, failing to fall within a statutory category of invention.

For purposes of examination, Claim 18 is being treated as the combination of software program and medium, not just the program itself. Claim 18 would be directed to an appropriate Manufacture within the meaning of 101 if the medium would only reasonably be interpreted by one of ordinary skill in the art as covering embodiments which are **articles produced from raw or prepared materials and which are structurally and functionally interconnect to the program in such a manner as to enable the program to act as a computer component and realize its functionality**. The “**computer readable medium**” in claim 18 would fairly suggest to one of ordinary skill signals or other forms of propagation and transmission media, typewritten or handwritten text on paper, or other items failing to be an appropriate manufacturer under 35 USC 101 in the **context of computer-related inventions**. Therefore, Claim 18 is rejected under 101 as failing to be limited to embodiments which fall within a statutory category.

### ***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Chandra et al. (Hereinafter referred to as Chandra, US Pat. No.: 7,130,885) in view of Hamada (**Dynamic role creation from role class hierarchy-security management of service session in dynamic service environment** Hamada, T.; Global Convergence of Telecommunications and Distributed Object Computing, 1997, Proceedings, TINA 97 17-20 Nov 1997 Page(s):152 - 163 Digital Object Identifier 10.1109/TINA.1997.660720).

As per claim 1:

Chandra discloses a method of achieving context-sensitive confidentiality among security domains, the method comprising steps of:

determining a route to be taken by a message to be transmitted where the route spans a plurality of the security domains (column 89: lines 60-67; column 91: lines 21-29; column 92: lines 36-50; column 93: lines 45-61);

determining rights of nodes to be encountered on the determined route to access security-sensitive portions of the message (column 74: lines 1-7, lines 19-26, lines 60-67; column 77: lines 13-24, lines 31-38, 0084);

selectively protecting the security-sensitive portions of the message, according to the determined access rights (column 74: lines 1-7, lines 19-26, lines 59-67, column 78: lines 12-33, 51-64); and  
transmitting the message with its selectively-protected portions on the determined route (column 74: lines 1-7, lines 19-26, lines 59-67, column 75: lines 26-44; column 78: lines 12-33, 51-64).

Chandra does not explicitly teach the security domains are within a federated environment. Hamada, in an analogous art, however teaches the security domains are within a federated environment (Section 5.3: Security space; Figure 5-1. Domain Layering and security space; Figure 3-2. Service Session, Service Transaction and Security Space Representation). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chandra to include the security domains are within a federated environment. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a systematic approach towards using role-hierarchy and algebraic operations on roles for strongly-role based and role-mapping between federated domains, within which complexity of security management in federation and composition can be made manageable as suggested by Hamada (in Section 1: Introduction; Last Paragraph).

As per claim 2:

Chandra discloses a method, wherein the selectively protecting step further comprises the step of encrypting at least one security-sensitive portion of the message (Column 76: 41-64).

As per claim 3:

Chandra discloses a method, wherein the selectively protecting step further comprises the step of computing a digital signature over at least one security-sensitive portion of the message (Column 77: lines 46-64; Column 78: lines 1-4).

As per claim 4:

Chandra discloses a method, wherein the step of determining the route further comprises the step of consulting policy to determine the route to be taken for this message (Column 75: lines 26-44; Column 76: 41-50).

As per claim 5:

Hamada discloses a method, wherein the step of determining the access rights further comprises the step of consulting policy for each of the nodes to be encountered (Section 4.4: Roles and access Privileges; Section 6.1: Role Class Hierarchy; Section 7.1: Role mapping in Federation).

As per claim 6:

Hamada discloses a method, comprising the step of determining a role of at least one of the nodes to be encountered, and wherein the step of determining the access rights further

comprises the step of consulting policy for each determined role, wherein the policy specifies access rights for that role (Section 4.4: Roles and access Privileges; Section 6.1: Role Class Hierarchy; Section 7.1: Role mapping in Federation).

As per claim 7:

Chandra discloses a method, wherein the selectively protecting step further comprises the step of encrypting each security-sensitive portion of the message for each node determined to have access rights to that portion (Claim 78: lines 51-64).

As per claim 8:

Chandra discloses a method, wherein the encrypting step uses a public key associated with each of the nodes for which the encrypting step operates (Column 76: 41-64).

As per claim 9:

Chandra discloses a method, wherein the determined route is specified in the transmitted message (Column 78: lines 51-64; Column 89: lines 60-67; column 91: lines 21-29; Column 92: lines 36-50; Column 93: lines 45-61).

As per claim 10:

Chandra discloses a method, wherein the step of determining a role of at least one of the nodes to be encountered, and wherein the selectively protecting step further comprises the step of

encrypting each security-sensitive portion of the message for each of the roles that are determined to have access rights to that portion (column 78: lines 12-33, 51-64).

As per claim 11:

Chandra discloses a method, wherein the encrypting step uses a public key associated with each of the roles for which the encrypting step operates column (column 75: lines 26-44, 55-67; 78: lines 12-33, 51-64).

As per claim 12:

Chandra discloses a method, wherein the steps of: receiving the transmitted message at a selected one of the nodes on the determined route; and securely accessing only those ones of the selectively-protected portions of the received message to which the selected node has access rights (column 74: lines 1-7, lines 19-26, lines 59-67, column 75: lines 26-44; column 78: lines 12-33, 51-64).

As per claim 13;

Chandra discloses a method, wherein the transmitted message contains information identifying an authentication authority from a first of the security domains, and indicates that this authentication authority has already authenticated a party for which the message requests access to services, such that nodes receiving the message in other ones of the security domains can bypass authentication of the party for access to services of that other security domain, upon verifying authenticity of the authentication authority and establishing that the authentication

authority vouches for the received message (column 74: lines 1-7, lines 19-26, lines 59-67, column 75: lines 26-44; column 77: lines 45-64; column 78: lines 12-33, 51-64; Column 80: lines 10-16, 29-36).

As per claim 14:

Chandra discloses a method, wherein the authentication authority is determined to vouch for the received message if a digital signature computed by the authentication authority and transmitted with the message is determined, by the node receiving the message in the one of the other security domains, to be valid (column 74: lines 1-7, lines 19-26, lines 59-67, column 75: lines 26-44; column 77: lines 45-64; column 78: lines 12-33, 51-64; Column 80: lines 10-16, 29-36).

As per claim 15:

Chandra discloses a method, wherein the transmitted message contains security credentials of the party, where those security credentials have been authenticated by the identified authentication authority and are protected such that only authorized ones of the nodes receiving the message in other ones of the security domains can access the protected security credentials (column 74: lines 1-7, lines 19-26, lines 59-67, column 75: lines 26-44; column 77: lines 45-64; column 78: lines 12-33, 51-64; Column 80: lines 10-16, 29-36).

As per claim 16:

Chandra discloses a method, wherein the protected security credentials are encrypted using a public key of each of the authorized ones of the nodes receiving the message, such that each of the authorized ones can decrypt the protected security credentials using a corresponding private key (column 74: lines 1-7, lines 19-26, lines 59-67, column 75: lines 26-44, 55-67; column 77: lines 45-64; column 78: lines 12-33, 51-64; Column 80: lines 10-16, 29-36).

As per claim 17:

Chandra discloses a system for achieving context-sensitive confidentiality among security domains, the system comprising:

means for determining a route to be taken by a message to be transmitted, where the route spans a plurality of the security domains (column 89: lines 60-67; column 91: lines 21-29; column 92: lines 36-50; column 93: lines 45-61);

means for determining rights of nodes to be encountered on the determined route to access security-sensitive portions of the message (column 74: lines 1-7, lines 19-26, lines 60-67; column 77: lines 13-24, lines 31-38, 0084);

means for selectively protecting the security-sensitive portions of the message, according to the determined access rights (column 74: lines 1-7, lines 19-26, lines 59-67, column 78: lines 12-33, 51-64); and

means for transmitting the message with its selectively-protected portions on the determined route (column 74: lines 1-7, lines 19-26, lines 59-67, column 75: lines 26-44; column 78: lines 12-33, 51-64).

Chandra does not explicitly teach the security domains are within a federated environment. Hamada, in an analogous art, however teaches the security domains are within a federated environment (Section 5.3: Security space; Figure 5-1. Domain Layering and security space; Figure 3-2. Service Session, Service Transaction and Security Space Representation). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chandra to include the security domains are within a federated environment. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a systematic approach towards using role-hierarchy and algebraic operations on roles for strongly-role based and role-mapping between federated domains, within which complexity of security management in federation and composition can be made manageable as suggested by Hamada (in Section 1: Introduction; Last Paragraph).

As per claim 18:

Chandra discloses a computer program product for securely transmitting context-sensitive confidential message content among security domains, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for determining a route to be taken by a message to be transmitted, where the route spans a plurality of the security domains (column 89: lines 60-67; column 91: lines 21-29; column 92: lines 36-50; column 93: lines 45-61);

computer-readable program code means for determining rights of nodes to be encountered on the determined route to access security-sensitive portions of the message (column 74: lines 1-7, lines 19-26, lines 60-67; column 77: lines 13-24, lines 31-38, 0084);

computer-readable program code means for selectively protecting the security-sensitive portions of the message, according to the determined access rights (column 74: lines 1-7, lines 19-26, lines 59-67, column 78: lines 12-33, 51-64); and

computer-readable program code means for transmitting the message with its selectively-protected portions on the determined route (column 74: lines 1-7, lines 19-26, lines 59-67, column 75: lines 26-44; column 78: lines 12-33, 51-64).

Chandra does not explicitly teach the security domains are within a federated environment. Hamada, in an analogous art, however teaches the security domains are within a federated environment (Section 5.3: Security space; Figure 5-1. Domain Layering and security space; Figure 3-2. Service Session, Service Transaction and Security Space Representation). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chandra to include the security domains are within a federated environment. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a systematic approach towards using role-hierarchy and algebraic operations on roles for strongly-role based and role-mapping between federated domains, within which complexity

of security management in federation and composition can be made manageable as suggested by Hamada (in Section 1: Introduction; Last Paragraph).

As per claim 19:

Chandra discloses a method of providing a message confidentiality service for securely transmitting messages among security domains, the method comprising steps of:

determining a route to be taken by a message to be transmitted, where the route spans a plurality of the security domains (column 89: lines 60-67; column 91: lines 21-29; column 92: lines 36-50; column 93: lines 45-61);

determining rights of nodes to be encountered on the determined route to access security-sensitive portions of the message (column 74: lines 1-7, lines 19-26, lines 60-67; column 77: lines 13-24, lines 31-38, 0084); and

determining how the security-sensitive portions of the message should be protected, according to the determined access rights (column 74: lines 1-7, lines 19-26, lines 59-67, column 78: lines 12-33, 51-64).

Chandra does not explicitly teach the security domains are within a federated environment. Hamada, in an analogous art, however teaches the security domains are within a federated environment (Section 5.3: Security space; Figure 5-1. Domain Layering and security space; Figure 3-2. Service Session, Service Transaction and Security Space Representation). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chandra to include the security

domains are within a federated environment. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a systematic approach towards using role-hierarchy and algebraic operations on roles for strongly-role based and role-mapping between federated domains, within which complexity of security management in federation and composition can be made manageable as suggested by Hamada (in Section 1: Introduction; Last Paragraph).

As per claim 20:

Hamada discloses a method, wherein the step of charging a fee for one or more of the determining steps (Section 8.2: Flexible Billing Management).

As per claim 21:

Chandra discloses a method, wherein the step of applying the determined protections to the security-sensitive portions (column 74: lines 1-7, lines 19-26, lines 59-67, column 78: lines 12-33, 51-64).

### ***Conclusion***

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art

***Contact Information***

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T.G/

April 11, 2008

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137